


JC17 Rec'd PCT/PTO 3 1 MAY 2001

FORM PTO-1390 US DEPARTMENT OF COMMERCE REV. 5-93 PATENT AND TRADEMARK OFFICE <b>TRANSMITTAL LETTER TO THE UNITED STATES          DESIGNATED/ELECTED OFFICE (DO/EO/US)          CONCERNING A FILING UNDER 35 U.S.C. 371</b>		ATTORNEYS DOCKET NUMBER <b>P01,0183</b>
		U.S. APPLICATION NO. (if known use 37 CFR 1.5) <b>09/857153</b>
INTERNATIONAL APPLICATION NO. <b>PCT/EP99/09496</b>	INTERNATIONAL FILING DATE <b>04 DECEMBER 1999</b>	PRIORITY DATE CLAIMED <b>04 DECEMBER 1998</b>
TITLE OF INVENTION <b>METHOD OF SECURE DATA TRANSMISSION</b>		
APPLICANT(S) FOR DO/EO/US <b>Klaus David GRADISCHNIG et al</b>		
Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:		
<ol style="list-style-type: none"> <li>1. <input checked="" type="checkbox"/> This is a <b>FIRST</b> submission of items concerning a filing under 35 U.S.C. 371.</li> <li>2. <input type="checkbox"/> This is a <b>SECOND</b> or <b>SUBSEQUENT</b> submission of items concerning a filing under 35 U.S.C. 371.</li> <li>3. <input checked="" type="checkbox"/> This express request to begin national examination procedures (35 U.S.C. 371(f)) at any time rather than delay.</li> <li>4. <input checked="" type="checkbox"/> A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.</li> <li>5. <input checked="" type="checkbox"/> A copy of International Application as filed (35 U.S.C. 371(c)(2)).           <ol style="list-style-type: none"> <li>a. <input checked="" type="checkbox"/> is transmitted herewith (required only if not transmitted by the International Bureau).</li> <li>b. <input type="checkbox"/> has been transmitted by the International Bureau.</li> <li>c. <input type="checkbox"/> is not required, as the application was filed in the United States Receiving Office (RO/US)</li> </ol> </li> <li>6. <input checked="" type="checkbox"/> A translation of the International Application into English (35 U.S.C. 371(c)(2)).</li> <li>7. <input checked="" type="checkbox"/> Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. §371(c)(3))           <ol style="list-style-type: none"> <li>a. <input type="checkbox"/> are transmitted herewith (required only if not transmitted by the International Bureau).</li> <li>b. <input type="checkbox"/> have been transmitted by the International Bureau.</li> <li>c. <input type="checkbox"/> have not been made; however, the time limit for making such amendments has NOT expired.</li> <li>d. <input checked="" type="checkbox"/> have not been made and will not be made.</li> </ol> </li> <li>8. <input type="checkbox"/> A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).</li> <li>9. <input checked="" type="checkbox"/> An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).</li> <li>10. <input type="checkbox"/> A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).</li> </ol>		
<b>Items 11. to 16. below concern other document(s) or information included:</b>		
11. <input checked="" type="checkbox"/> An Information Disclosure Statement under 37 C.F.R. 1.97 and 1.98; (PTO 1449, Prior Art, Search Report, 05 References).		
12. <input checked="" type="checkbox"/> An assignment document for recording. A separate cover sheet in compliance with 37 C.F.R. 3.28 and 3.31 is included. <b>(SEE ATTACHED ENVELOPE)</b>		
13. <input checked="" type="checkbox"/> Amendment "A" Prior to Action and Appendix "A". <input type="checkbox"/> A SECOND or SUBSEQUENT preliminary amendment.		
14. <input checked="" type="checkbox"/> A substitute specification and substitute specification mark-up.		
15. <input checked="" type="checkbox"/> A change of address letter attached to the Declaration.		
16. <input checked="" type="checkbox"/> Other items or information: <ol style="list-style-type: none"> <li>a. <input checked="" type="checkbox"/> Submission of Drawings and drawing changes</li> <li>b. <input checked="" type="checkbox"/> Appointment of Associate Power of Attorney</li> <li>c. <input checked="" type="checkbox"/> EXPRESS MAIL #EL 843728230 US dated May 31, 2001</li> </ol>		

U.S. APPLICATION NO. (if known, use 37 C.F.R. 1.51) <b>09/857153</b>		INTERNATIONAL APPLICATION NO. <b>PCT/EP99/09496</b>		ATTORNEY'S DOCKET NUMBER <b>P01,0183</b>	
17. <input checked="" type="checkbox"/> The following fees are submitted:  <b>BASIC NATIONAL FEE (37 C.F.R. 1.492(a)(1)-(5):</b> Search Report has been prepared by the EPO or JPO \$860.00  International preliminary examination fee paid to USPTO (37 C.F.R. 1.482) \$690.00  No international preliminary examination fee paid to USPTO (37 C.F.R. 1.482) but international search fee paid to USPTO (37 C.F.R. 1.445(a)(2)) \$710.00  Neither international preliminary examination fee (37 C.F.R. 1.482) nor international search fee (37 C.F.R. 1.445(a)(2)) paid to USPTO \$1000.00  International preliminary examination fee paid to USPTO (37 C.F.R. 1.482) and all claims satisfied provisions of PCT Article 33(2)-(4) \$ 100.00  <div style="text-align: right;"><b>ENTER APPROPRIATE BASIC FEE AMOUNT =</b></div>				CALCULATIONS	PTO USE ONLY
Surcharge of \$130.00 for furnishing the oath or declaration later than <input type="checkbox"/> 20 <input type="checkbox"/> 30 months from the earliest claimed priority date (37 C.F.R. 1.492(e)).				\$	
Claims	Number Filed	Number Extra	Rate		
Total Claims	04 - 20 =	0	X \$ 18.00	\$	
Independent Claims	04 - 3 =	1	X \$ 80.00	\$ 80.00	
Multiple Dependent Claims			\$270.00 +	\$	
<b>TOTAL OF ABOVE CALCULATIONS =</b>				\$ 940.00	
Reduction by 1/2 for filing by small entity, if applicable. Verified Small Entity statement must also be filed. (Note 37 C.F.R. 1.9, 1.27, 1.28)				\$	
<b>SUBTOTAL =</b>				\$ 940.00	
Processing fee of \$130.00 for furnishing the English translation later than <input type="checkbox"/> 20 <input type="checkbox"/> 30 months from the earliest claimed priority date (37 CFR 1.492(f)) +				\$	
<b>TOTAL NATIONAL FEE =</b>				\$ 940.00	
Fee for recording the enclosed assignment (37 C.F.R. 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 C.F.R. 3.28, 3.31). \$40.00 per property +					
<b>TOTAL FEES ENCLOSED =</b>				\$ 940.00	
				Amount to be refunded	\$
				charged	\$
a. <input checked="" type="checkbox"/> A check in the amount of \$ <u>940.00</u> to cover the above fees is enclosed.  b. <input type="checkbox"/> Please charge my Deposit Account No. _____ in the amount of \$ _____ to cover the above fees. A duplicate copy of this sheet is enclosed.  c. <input checked="" type="checkbox"/> The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. <b>50-1519</b> . <b>A duplicate copy of this sheet is enclosed.</b> NOTE: Where an appropriate time limit under 37 C.F.R. 1.494 or 1.495 has not been met, a petition to revive (37 C.F.R. 1.137(a) or (b)) must be filed and granted to restore the application to pending status.					
<u><b>SEND ALL CORRESPONDENCE TO:</b></u>  <div style="display: flex; justify-content: space-between;"> <div style="width: 40%;"> <b>SCHIFF HARDIN &amp; WAITE</b>  <b>PATENT DEPARTMENT</b>  <b>6600 Sears Tower</b>  <b>233 South Wacker Drive</b>  <b>Chicago, Illinois 60606-6473</b> </div> <div style="width: 40%; text-align: center;">             SIGNATURE      MARK BERGNER      (REG. NO. 45,877)         </div> <div style="width: 20%; text-align: center;">           DATE: May 31, 2001         </div> </div>					
<b>CUSTOMER NUMBER 26574</b>					

# SPECIFICATION

## TITLE

### METHOD OF SECURE DATA TRANSMISSION

#### BACKGROUND OF THE INVENTION

##### 5 Field of the Invention

[0001] The invention relates to a method of transmitting data securely in which redundant messages are transmitted.

##### Description of the Related Art

10 [0002] Many transmission media/protocols have a transmit-receive property in which messages transferred to a medium by the transmitter arrive at the receiver in the same way (assuming that they arrive at all) that they were transmitted. In other words, message overhaul does not take place. Many protocols ensuring secure message transmission have this transmit-receive property as a prerequisite for the underlying transmission media/protocols which they use, since this transmit-receive property makes it much simpler to ensure efficient, secure message transmission. 15 Historically, there has been a problem of defining protocols for secure message transmission which do not require this transmit-receive property (i.e., possibly having message overhaul).

20 [0003] The following methods are (or may be) used for the purpose of defining such protocols. Although a prerequisite of the MTP standard (cf. Q.700 to Q.706) involves transmission media on which message overhaul cannot take place, MTP Level 2 (Q.703) is also able to operate with transmission media which do not have the transmit-receive property.

25 [0004] It is fundamental to the operation of the protocol (Basic Error Correction), even in the case of message overhaul, that the MTP recognizes after a retransmission request whether a particular message has been sent on the basis of the retransmission request (it is then accepted), or whether it was actually sent before the retransmission request (it is then discarded). However, a disadvantage of this protocol is that it has no selective retransmission mode, which can be inefficient.

In addition, without modification of MTP Level 2, the entire available bandwidth would be used, which may be disadvantageous.

[0005] MTP Level 2 with the Preventive Cyclic Retransmission method can also operate with message overhaul, since no retransmission requests are generated and messages which do not arrive in the correct order are discarded. Again, the disadvantage of the method is a poor utilization of the bandwidth.

[0006] TCP, which uses IP as underlying network protocol, has also solved the problem. Transmitted blocks which are not acknowledged are retransmitted when a timer has run out. This protocol mechanism (in which only blocks received without gaps are acknowledged) results in unnecessary retransmissions, depending on the round trip delay (even if the acknowledgement timeout is chosen to be long enough) since the acknowledgement timer often also runs out for messages which have been received correctly after a lost message.

[0007] The situation is improved somewhat by methods such as Fast Retransmission and providing an explicit NACK upon the first occurrence of a gap.

[0008] The Reliable Data protocol works in a similar way to TCP, with the extension that messages which are not received without gaps can also be acknowledged.

#### SUMMARY OF THE INVENTION

[0009] The present invention extends and modifies certain existing protocols in order to ensure efficient, secure data transmission using transmission media and protocols in which message overhaul can take place.

[0010] In this context, the present invention is based on the realization that, for a modern protocol which is intended to work efficiently (i.e., more rapidly) using a transmission medium/protocol with possible message overhaul, and having loss detection with minimization of unnecessarily transmitted information, the following properties are advantageous:

- a) multiple selective retransmission method without full dependency on a timer; specifically, the loss of an ACK should not result in retransmission,

- b) explicit status alignment between a transmitter and receiver,
- c) retransmission of a message only if there is a certain probability that the message is lost,
- d) messages received a plurality of times must not cause an incorrect response, and
- e) use of parameter value selection to determine the tradeoff between rapid error correction and minimum unnecessary message transmission.

[0011] The most important of these points is point (d). Specifically, there are two opportunities/situations for messages received more than once to cause incorrect responses:

- i) the message is recognized as having already been received, and this is defined as an error in accordance with the protocol; and
- ii) the message is interpreted as a new message and triggers an action which later results in an error being detected in a transmitter or receiver as a consequence. By way of example, a supposed message loss may be detected by virtue of such a message. This results in a retransmission request for messages which have not actually been sent yet, which is interpreted as an error by the transmitter.

[0012] One option for guaranteeing item (d) in protocols which satisfy the other items sufficiently, but not item (d), is for a message transmitted for the second time or more to be specially marked. Such protocols can then easily be changed so that such marked messages are simply ignored in the situations described under (i) and (ii).

[0013] Another opportunity to eliminate situation (i) is to ignore such messages as a general rule.

[0014] For situation (ii), a window can also be defined so that messages received outside of this window are generally ignored and do not result in any retransmission requests.

## BRIEF DESCRIPTION OF THE DRAWINGS

[0015] Exemplary embodiments of the invention are explained in more detail with the aid of figures.

- 5            Figure 1        is a data structure diagram showing the structure of the Sequenced Data Protocol Data Unit (SD-PDU) according to prior art Figure 3 of the ITU-T Recommendation Q.2110;
- Figure 2        is a data structure diagram showing the structure of the Poll Protocol Data Unit (SD-PDU) according to prior art Figure 4 of the ITU-T Recommendation Q.2110;
- 10           Figure 3        is a data structure diagram showing the structure of the Sequenced Data Protocol Data Unit (SD-PDU) according to prior art Figure 5 of the ITU-T Recommendation Q.2110;
- Figures 4A & 4B    are flowchart segments showing the SSCOP processing according to Figure 20, sheet 40 of 51, of the ITU-T Recommendation Q.2110 as modified by method 1 of the present invention;
- 15           Figures 5A & 5B    are flowchart segments showing the SSCOP processing according to Figure 20, sheet 43 of 51, of the ITU-T Recommendation Q.2110 as modified by method 1 of the present invention;
- 20           Figures 6A & 6B    are flowchart segments showing the SSCOP processing according to Figure 20, sheet 44 of 51, of the ITU-T Recommendation Q.2110 as modified by method 1 of the present invention;
- 25           Figures 7A & 7B    are flowchart segments showing the SSCOP processing according to Figure 20, sheet 40 of 51, of the ITU-T Recommendation Q.2110 as modified by method 2 of the present invention; and
- 30           Figure 8        is a flowchart segments showing the SSCOP processing according to common elements of Figure 20, from sheets 40, 41, 43 and 44 of 51, of the ITU-T Recommendation Q.2110.

## DETAILED DESCRIPTION OF THE INVENTION

[0016] The exemplary embodiment chosen is the protocol Service Specific Connection-Oriented Protocol (SSCOP) described in ITU-T Recommendation Q.2110 (07/94) - B-ISDN ATM ADAPTATION LAYER - SERVICE SPECIFIC CONNECTION ORIENTED PROTOCOL (SSCOP) Q.2110 (herein incorporated by reference). This protocol fulfills the properties (a) through (c) identified above, but has the problems described under (i) and (ii). Specifically, when the message is recognized as having already been received and this is defined as an error in accordance with the protocol (i), this results in an incorrect response (branch to the connector D) in ITU-T Rec. Q.2110 (Figure 4B). Similarly, Figures 4A and 4B show that a message having the property described in (ii) usually results in a retransmission request (USTAT). This in turn usually results in a branch to the error branch (connector D) in Figure 5B.

[0017] In one embodiment of the invention, method 1, in accordance with the discussion above, a Sequenced Data Protocol Data Unit (SD-PDU) is now specially marked in the case of repeated transmission, e.g., by setting bit 5 in the PDU trailer (Figure 1, the RX field) to 1 (Figure 5A, 5.1), indicating a repeated transmission. This embodiment modifies the ITU-T Rec. Q.2110, Figure 20 (sheet 40 of 51) such that, in the two error situations described above, a check is first carried out to determine whether the SD-PDU is marked as having been repeated (Figure 4A, 4.1). In this case, the message is ignored and an incorrect response cannot occur.

[0018] Alternatively, in method 2, the ITU-T Rec. Q.2110 figure 20 (sheet 40 of 51) is modified such that the error case (i) is generally not checked, and a message which has already been received is simply ignored (Figure 7B, 7.2, TRUE path). In addition, likewise in Figure 7A, the ITU-T Rec. Q.2110 figure 20 (sheet 40 of 51) is modified such that, after the query  $VR(H) < VR(MR)$ , a check is carried out to determine whether  $SD.N(S) < VR(R) + 2^{23}$ , for example (Figure 7B, 7.2). (This presupposes that the window size used for the flow control is always smaller than  $2^{23}$ , which does not represent any relevant restriction, however). If this is not the case, the message is discarded (Figure 7A, 7.1, FALSE path), otherwise it is handled as previously.

[0019] Item (e) can also easily be achieved with SSCOP, e.g., USTATs could be sent only with a certain time delay, in order to wait for messages which have

been repeated. In addition, it would be possible for only gaps which have already existed for a certain time to be reported (or heeded) using/in the case of a STAT.

[0020] The above-described methods are illustrative of the principles of the present invention. Numerous modifications and adaptations will be readily apparent to those skilled in this art without departing from the spirit and scope of the present invention.

5



## ABSTRACT

[0021] The invention shows how certain existing protocols can be enlarged/modified in order to guarantee an efficient, secure data transmission via transmission media/protocols, whereby message overhaul can occur. The invention  
5 relates to a method by way of which a message, which has been transmitted for at least the second time, is particularly marked by the transmitter. The message which is marked as transmitted for at least the second time is ignored by the receiver when the message has already been received or is new.

10  
15  
20  
25  
30  
35  
40  
45  
50  
55  
60  
65  
70  
75  
80  
85  
90  
95  
100  
105  
110  
115  
120  
125  
130  
135  
140  
145  
150  
155  
160  
165  
170  
175  
180  
185  
190  
195  
200  
205  
210  
215  
220  
225  
230  
235  
240  
245  
250  
255  
260  
265  
270  
275  
280  
285  
290  
295  
300  
305  
310  
315  
320  
325  
330  
335  
340  
345  
350  
355  
360  
365  
370  
375  
380  
385  
390  
395  
400  
405  
410  
415  
420  
425  
430  
435  
440  
445  
450  
455  
460  
465  
470  
475  
480  
485  
490  
495  
500  
505  
510  
515  
520  
525  
530  
535  
540  
545  
550  
555  
560  
565  
570  
575  
580  
585  
590  
595  
600  
605  
610  
615  
620  
625  
630  
635  
640  
645  
650  
655  
660  
665  
670  
675  
680  
685  
690  
695  
700  
705  
710  
715  
720  
725  
730  
735  
740  
745  
750  
755  
760  
765  
770  
775  
780  
785  
790  
795  
800  
805  
810  
815  
820  
825  
830  
835  
840  
845  
850  
855  
860  
865  
870  
875  
880  
885  
890  
895  
900  
905  
910  
915  
920  
925  
930  
935  
940  
945  
950  
955  
960  
965  
970  
975  
980  
985  
990  
995

BOX PCT  
IN THE UNITED STATES DESIGNATED/ELECTED OFFICE  
OF THE UNITED STATES PATENT AND TRADEMARK OFFICE  
UNDER THE PATENT COOPERATION TREATY--CHAPTER II

5                                    **PRELIMINARY AMENDMENT A**  
                                         **PRIOR TO ACTION**

APPLICANT(S):                                    Klaus David GRADISCHNIG et al  
ATTORNEY DOCKET NO.:                        P01,0183  
INTERNATIONAL APPLICATION NO:            PCT/EP99/09496  
INTERNATIONAL FILING DATE:                04 December 1999  
INVENTION:    METHOD OF SECURE DATA TRANSMISSION

Assistant Commissioner for Patents,  
Washington D.C. 20231

10                                   Sir:

Applicants herewith amend the above-referenced PCT application, and  
request entry of the Amendment prior to examination on the United States  
Examination Phase.

15                                   **IN THE CLAIMS:**

On page 6:

replace line 1 with --WHAT IS CLAIMED IS:--;

Please replace original claims 1-4 with the following rewritten claims 1-4,  
referring to the mark-ups in Appendix A.

20                                   1. (Amended) A method of secure data transmission which is executed on a  
layer basis using a transmission method having possible message overhaul,  
comprising the steps of:

25                                   specially marking a message which is already being transmitted for at least a  
second time by said transmitter; and

ignoring said message which is marked as having been transmitted for at  
least a second time by a receiver if it recognizes said message as having already  
been received or if it interprets said message as a new message.

2. (Amended) A method of secure data transmission wherein a transmitter protocol operates on a layer basis using a transmitter protocol having possible message overhaul, comprising the steps of:

5 specially marking, by said transmitter protocol, a message which is already being transmitted for at least a second time.

3. (Amended) A method of secure data transmission wherein a receiver protocol operates on a layer basis using a receiver protocol having possible message overhaul, comprising the steps of:

10 ignoring, by said receiver protocol, a message which is marked as having been transmitted at least for a second time if it recognizes the message as having already been received or if it interprets said message as a new message.

4. (Amended) A method of secure data transmission wherein a receiver protocol operates on a layer basis using a receiver protocol having possible message overhaul, comprising the steps of:

15 ignoring, by said receiver protocol, a message if it recognizes said message as having already been received or if, although it interprets said message as a new message, said message is situated outside of a prescribed window.

#### 20 REMARKS

The present Amendment revises the specification and claims to conform to United States patent practice, before examination of the present PCT application in the United States National Examination Phase. Pursuant to 37 CFR 1.125 (b), applicants have concurrently submitted a substitute specification, excluding the  
25 claims, and provided a marked-up copy. All of the changes are editorial and applicant believes no new matter is added thereby. The amendment, addition, and/or cancellation of claims is not intended to be a surrender of any of the subject matter of those claims.

Early examination on the merits is respectfully requested.

Submitted by,

(Reg. No. 45,877)

Mark Bergner  
Schiff Hardin & Waite  
Patent Department  
6600 Sears Tower  
233 South Wacker Drive  
Chicago, Illinois 60606-6473  
(312) 258-5779  
Attorneys for Applicant

**CUSTOMER NUMBER 26574**

Appendix A  
Mark Ups for Claim Amendments

1. **(Amended)** A method of secure data transmission which is executed on a layer basis using a transmission method ~~[with]~~**having** possible message overhaul, **comprising the steps of:**

~~[characterized in that]~~

(a) ~~]~~**specially marking** a message which is already being transmitted for at least ~~[the]~~**a** second time ~~[is specially marked]~~ by ~~[the]~~**said** transmitter~~[-]~~; **and**

(b) ~~—~~**a**~~]~~**ignoring said** message which is marked as having been transmitted for at least ~~[the]~~**a** second time ~~[is ignored]~~ by ~~[the]~~**a** receiver if it recognizes ~~[the]~~**said** message as having already been received or if it interprets ~~[the]~~**said** message as a new message.

2.~~[-A]~~ **(Amended) A method of secure data transmission wherein a** transmitter protocol~~[-which]~~ operates on a layer basis using a transmitter protocol ~~[with]~~**having** possible message overhaul, **comprising the steps of:**

~~[characterized in that]~~

~~[it]~~~~]~~~~specially [marks]~~**marking, by said transmitter protocol,** a message which is already being transmitted for at least ~~[the]~~**a** second time.

3.~~[-A]~~ **(Amended) A method of secure data transmission wherein a** receiver protocol~~[-which]~~ operates on a layer basis using a receiver protocol ~~[with]~~**having** possible message overhaul, **comprising the steps of:**

~~[characterized in that]~~

~~[it ignores]~~**ignoring, by said receiver protocol,** a message which is marked as having been transmitted at least for ~~[the]~~**a** second time if it recognizes the message as having already been received or if it interprets ~~[the]~~**said** message as a new message.

4.~~[-A]~~ **(Amended) A method of secure data transmission wherein a** receiver protocol~~[-which]~~ operates on a layer basis using a receiver protocol ~~[with]~~**having** possible message overhaul, **comprising the steps of:**  
~~[characterized in that]~~

[it ignores]ignoring, by said receiver protocol, a message if it recognizes [the]said message as having already been received or if, although it interprets [the]said message as a new message, [this]said message is situated outside of a prescribed window.

5

Document comparison done by DeltaView on Wednesday, May 09, 2001 10:11:19

Input:	
Document 1	file:///Q:/documents/Year 2001/p010183-gradsechnig-secure data transmission/original claims.doc
Document 2	file:///Q:/documents/Year 2001/p010183-gradsechnig-secure data transmission/amended claims.doc
Rendering set	Mark PTO

Legend:	
<u>Insertion</u>	
[Deletion]	
[Moved from]	
<u>Moved to</u>	
Format change	
Inserted cell	
Deleted cell	
Moved cell	
Split/Merged cell	
Padding cell	

Statistics:		
	Count	% of content
Insertions	31	25.16%
Deletions	35	12.03%
Moves	0	0.00%
Matched	32	62.81%
Format changed	0	0.00%

10

BOX PCT  
IN THE UNITED STATES DESIGNATED/ELECTED OFFICE  
OF THE UNITED STATES PATENT AND TRADEMARK OFFICE  
UNDER THE PATENT COOPERATION TREATY--CHAPTER II

**REQUEST FOR APPROVAL OF DRAWING CHANGES**

APPLICANT(S): Klaus David GRADISCHNIG et al  
ATTORNEY DOCKET NO.: P01,0183  
INTERNATIONAL APPLICATION NO: PCT/EP99/09496  
INTERNATIONAL FILING DATE: 04 December 1999  
INVENTION: METHOD OF SECURE DATA TRANSMISSION

Assistant Commissioner for Patents,  
Washington, D.C. 20231

Sir:

Enclosed are eleven sheets of drawings showing in red, changes to the  
Figures. Approval of the changes is respectfully requested.

Submitted by,

(Reg. No. 45,877)

Mark Bergner  
SCHIFF HARDIN & WAITE  
PATENT DEPARTMENT  
6600 Sears Tower  
Chicago, Illinois 60606-6473  
(312) 258-5779  
Attorney for Applicant(s)

**CUSTOMER NUMBER 26574**

532 Rec'd PCT.TTO 31 MAY 2001

BOX PCT  
IN THE UNITED STATES DESIGNATED/ELECTED OFFICE  
OF THE UNITED STATES PATENT AND TRADEMARK OFFICE  
UNDER THE PATENT COOPERATION TREATY--CHAPTER II

**PRELIMINARY AMENDMENT A**  
**PRIOR TO ACTION**

APPLICANT(S): Klaus David GRADISCHNIG et al  
ATTORNEY DOCKET NO.: P01,0183  
INTERNATIONAL APPLICATION NO: PCT/EP99/09496  
INTERNATIONAL FILING DATE: 04 December 1999  
INVENTION: METHOD OF SECURE DATA TRANSMISSION

Assistant Commissioner for Patents,  
Washington D.C. 20231

Sir:

Applicants herewith amend the above-referenced PCT application, and request entry of the Amendment prior to examination on the United States Examination Phase.

**IN THE CLAIMS:**

On page 6:

replace line 1 with --WHAT IS CLAIMED IS:--;

Please replace original claims 1-4 with the following rewritten claims 1-4, referring to the mark-ups in Appendix A.

1. (Amended) A method of secure data transmission which is executed on a layer basis using a transmission method having possible message overhaul, comprising the steps of:

specially marking a message which is already being transmitted for at least a second time by said transmitter; and

ignoring said message which is marked as having been transmitted for at least a second time by a receiver if it recognizes said message as having already been received or if it interprets said message as a new message.



2. (Amended) A method of secure data transmission wherein a transmitter protocol operates on a layer basis using a transmitter protocol having possible message overhaul, comprising the steps of:

5 specially marking, by said transmitter protocol, a message which is already being transmitted for at least a second time.

3. (Amended) A method of secure data transmission wherein a receiver protocol operates on a layer basis using a receiver protocol having possible message overhaul, comprising the steps of:

10 ignoring, by said receiver protocol, a message which is marked as having been transmitted at least for a second time if it recognizes the message as having already been received or if it interprets said message as a new message.

4. (Amended) A method of secure data transmission wherein a receiver protocol operates on a layer basis using a receiver protocol having possible message overhaul, comprising the steps of:


15 ignoring, by said receiver protocol, a message if it recognizes said message as having already been received or if, although it interprets said message as a new message, said message is situated outside of a prescribed window.

20 **REMARKS**

The present Amendment revises the specification and claims to conform to United States patent practice, before examination of the present PCT application in the United States National Examination Phase. Pursuant to 37 CFR 1.125 (b), applicants have concurrently submitted a substitute specification, excluding the claims, and provided a marked-up copy. All of the changes are editorial and applicant believes no new matter is added thereby. The amendment, addition, and/or cancellation of claims is not intended to be a surrender of any of the subject matter of those claims.

Early examination on the merits is respectfully requested.

Submitted by,

 (Reg. No. 45,877)

Mark Bergner  
Schiff Hardin & Waite  
Patent Department  
6600 Sears Tower  
233 South Wacker Drive  
Chicago, Illinois 60606-6473  
(312) 258-5779  
Attorneys for Applicant

**CUSTOMER NUMBER 26574**

Appendix A  
Mark Ups for Claim Amendments

1. **(Amended)** A method of secure data transmission which is executed on a layer basis using a transmission method ~~[with]~~**having** possible message overhaul, **comprising the steps of:**

~~[characterized in that]~~

~~[a)]~~**specially marking** a message which is already being transmitted for at least ~~[the]~~**a** second time ~~[is specially marked]~~ by ~~[the]~~**said** transmitter~~]; and~~

~~[b)]~~**ignoring said** message which is marked as having been transmitted for at least ~~[the]~~**a** second time ~~[is ignored]~~ by ~~[the]~~**a** receiver if it recognizes ~~[the]~~**said** message as having already been received or if it interprets ~~[the]~~**said** message as a new message.

2.~~[-A]~~ **(Amended) A method of secure data transmission wherein a** transmitter protocol~~[-which]~~ operates on a layer basis using a transmitter protocol ~~[with]~~**having** possible message overhaul, **comprising the steps of:**

~~[characterized in that]~~

~~[it]~~**specially [marks] marking, by said transmitter protocol,** a message which is already being transmitted for at least ~~[the]~~**a** second time.

3.~~[-A]~~ **(Amended) A method of secure data transmission wherein a** receiver protocol~~[-which]~~ operates on a layer basis using a receiver protocol ~~[with]~~**having** possible message overhaul, **comprising the steps of:**

~~[characterized in that]~~

~~[it ignores]~~**ignoring, by said receiver protocol,** a message which is marked as having been transmitted at least for ~~[the]~~**a** second time if it recognizes the message as having already been received or if it interprets ~~[the]~~**said** message as a new message.

4.~~[-A]~~ **(Amended) A method of secure data transmission wherein a** receiver protocol~~[-which]~~ operates on a layer basis using a receiver protocol ~~[with]~~**having** possible message overhaul, **comprising the steps of:**  
~~[characterized in that]~~

[it ignores]ignoring, by said receiver protocol, a message if it recognizes [the]said message as having already been received or if, although it interprets [the]said message as a new message, [this]said message is situated outside of a prescribed window.

5

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37  
38  
39  
40  
41  
42  
43  
44  
45  
46  
47  
48  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59  
60  
61  
62  
63  
64  
65  
66  
67  
68  
69  
70  
71  
72  
73  
74  
75  
76  
77  
78  
79  
80  
81  
82  
83  
84  
85  
86  
87  
88  
89  
90  
91  
92  
93  
94  
95  
96  
97  
98  
99  
100  
101  
102  
103  
104  
105  
106  
107  
108  
109  
110  
111  
112  
113  
114  
115  
116  
117  
118  
119  
120  
121  
122  
123  
124  
125  
126  
127  
128  
129  
130  
131  
132  
133  
134  
135  
136  
137  
138  
139  
140  
141  
142  
143  
144  
145  
146  
147  
148  
149  
150  
151  
152  
153  
154  
155  
156  
157  
158  
159  
160  
161  
162  
163  
164  
165  
166  
167  
168  
169  
170  
171  
172  
173  
174  
175  
176  
177  
178  
179  
180  
181  
182  
183  
184  
185  
186  
187  
188  
189  
190  
191  
192  
193  
194  
195  
196  
197  
198  
199  
200  
201  
202  
203  
204  
205  
206  
207  
208  
209  
210  
211  
212  
213  
214  
215  
216  
217  
218  
219  
220  
221  
222  
223  
224  
225  
226  
227  
228  
229  
230  
231  
232  
233  
234  
235  
236  
237  
238  
239  
240  
241  
242  
243  
244  
245  
246  
247  
248  
249  
250  
251  
252  
253  
254  
255  
256  
257  
258  
259  
260  
261  
262  
263  
264  
265  
266  
267  
268  
269  
270  
271  
272  
273  
274  
275  
276  
277  
278  
279  
280  
281  
282  
283  
284  
285  
286  
287  
288  
289  
290  
291  
292  
293  
294  
295  
296  
297  
298  
299  
300  
301  
302  
303  
304  
305  
306  
307  
308  
309  
310  
311  
312  
313  
314  
315  
316  
317  
318  
319  
320  
321  
322  
323  
324  
325  
326  
327  
328  
329  
330  
331  
332  
333  
334  
335  
336  
337  
338  
339  
340  
341  
342  
343  
344  
345  
346  
347  
348  
349  
350  
351  
352  
353  
354  
355  
356  
357  
358  
359  
360  
361  
362  
363  
364  
365  
366  
367  
368  
369  
370  
371  
372  
373  
374  
375  
376  
377  
378  
379  
380  
381  
382  
383  
384  
385  
386  
387  
388  
389  
390  
391  
392  
393  
394  
395  
396  
397  
398  
399  
400  
401  
402  
403  
404  
405  
406  
407  
408  
409  
410  
411  
412  
413  
414  
415  
416  
417  
418  
419  
420  
421  
422  
423  
424  
425  
426  
427  
428  
429  
430  
431  
432  
433  
434  
435  
436  
437  
438  
439  
440  
441  
442  
443  
444  
445  
446  
447  
448  
449  
450  
451  
452  
453  
454  
455  
456  
457  
458  
459  
460  
461  
462  
463  
464  
465  
466  
467  
468  
469  
470  
471  
472  
473  
474  
475  
476  
477  
478  
479  
480  
481  
482  
483  
484  
485  
486  
487  
488  
489  
490  
491  
492  
493  
494  
495  
496  
497  
498  
499  
500  
501  
502  
503  
504  
505  
506  
507  
508  
509  
510  
511  
512  
513  
514  
515  
516  
517  
518  
519  
520  
521  
522  
523  
524  
525  
526  
527  
528  
529  
530  
531  
532  
533  
534  
535  
536  
537  
538  
539  
540  
541  
542  
543  
544  
545  
546  
547  
548  
549  
550  
551  
552  
553  
554  
555  
556  
557  
558  
559  
560  
561  
562  
563  
564  
565  
566  
567  
568  
569  
570  
571  
572  
573  
574  
575  
576  
577  
578  
579  
580  
581  
582  
583  
584  
585  
586  
587  
588  
589  
590  
591  
592  
593  
594  
595  
596  
597  
598  
599  
600  
601  
602  
603  
604  
605  
606  
607  
608  
609  
610  
611  
612  
613  
614  
615  
616  
617  
618  
619  
620  
621  
622  
623  
624  
625  
626  
627  
628  
629  
630  
631  
632  
633  
634  
635  
636  
637  
638  
639  
640  
641  
642  
643  
644  
645  
646  
647  
648  
649  
650  
651  
652  
653  
654  
655  
656  
657  
658  
659  
660  
661  
662  
663  
664  
665  
666  
667  
668  
669  
670  
671  
672  
673  
674  
675  
676  
677  
678  
679  
680  
681  
682  
683  
684  
685  
686  
687  
688  
689  
690  
691  
692  
693  
694  
695  
696  
697  
698  
699  
700  
701  
702  
703  
704  
705  
706  
707  
708  
709  
710  
711  
712  
713  
714  
715  
716  
717  
718  
719  
720  
721  
722  
723  
724  
725  
726  
727  
728  
729  
730  
731  
732  
733  
734  
735  
736  
737  
738  
739  
740  
741  
742  
743  
744  
745  
746  
747  
748  
749  
750  
751  
752  
753  
754  
755  
756  
757  
758  
759  
760  
761  
762  
763  
764  
765  
766  
767  
768  
769  
770  
771  
772  
773  
774  
775  
776  
777  
778  
779  
780  
781  
782  
783  
784  
785  
786  
787  
788  
789  
790  
791  
792  
793  
794  
795  
796  
797  
798  
799  
800  
801  
802  
803  
804  
805  
806  
807  
808  
809  
810  
811  
812  
813  
814  
815  
816  
817  
818  
819  
820  
821  
822  
823  
824  
825  
826  
827  
828  
829  
830  
831  
832  
833  
834  
835  
836  
837  
838  
839  
840  
841  
842  
843  
844  
845  
846  
847  
848  
849  
850  
851  
852  
853  
854  
855  
856  
857  
858  
859  
860  
861  
862  
863  
864  
865  
866  
867  
868  
869  
870  
871  
872  
873  
874  
875  
876  
877  
878  
879  
880  
881  
882  
883  
884  
885  
886  
887  
888  
889  
890  
891  
892  
893  
894  
895  
896  
897  
898  
899  
900  
901  
902  
903  
904  
905  
906  
907  
908  
909  
910  
911  
912  
913  
914  
915  
916  
917  
918  
919  
920  
921  
922  
923  
924  
925  
926  
927  
928  
929  
930  
931  
932  
933  
934  
935  
936  
937  
938  
939  
940  
941  
942  
943  
944  
945  
946  
947  
948  
949  
950  
951  
952  
953  
954  
955  
956  
957  
958  
959  
960  
961  
962  
963  
964  
965  
966  
967  
968  
969  
970  
971  
972  
973  
974  
975  
976  
977  
978  
979  
980  
981  
982  
983  
984  
985  
986  
987  
988  
989  
990  
991  
992  
993  
994  
995  
996  
997  
998  
999  
1000

98 P 5890 DE

## Description

## Method of secure data transmission

5 1. What technical problem is intended to be solved by your invention?

2. How has this problem been solved up until now?

3. In what way does your invention solve the specified technical problem?

10 4. Exemplary embodiment(s) of the invention.

1. Many transmission media/protocols have the property that messages transferred to the medium by the transmitter arrive at the receiver in the same way  
15 (assuming that they arrive) in which they were transmitted. In other words, message overhaul does not take place. Many protocols ensuring secure message transmission have this property as a prerequisite for the underlying transmission media/protocols which they  
20 use, since this property makes it much simpler to ensure efficient, secure message transmission. The problem now is that of defining protocols for secure message transmission which do not require this property.

25

2. The following methods are used for this purpose or may be used for this purpose: although a prerequisite of the MTP standard (cf. Q.700 to Q.706) is transmission media on which message overhaul cannot  
30 take place, MTP Level 2 (Q.703) is also able to operate with transmission media which do not have this property. It is fundamental to the operation of the protocol (Basic Error Correction), even in the case of message overhaul, that the MTP recognizes after a  
35 retransmission request whether a particular message has been sent on the basis of the retransmission request (it is then accepted), or whether it was actually

sent before the retransmission request (it is then discarded). However, a disadvantage of this protocol is that it has no selective retransmission mode, which can be inefficient. In addition, without modification of  
5 MTP Level 2, the entire available bandwidth would be used, which may be disadvantageous.

MTP Level 2 with Preventive Cyclic Retransmission method can also operate with message overhaul, since no  
10 retransmission requests are generated and messages which do not arrive in the correct order are discarded. The disadvantage of the method is again poor utilization of the bandwidth.

15 TCP, which uses IP as underlying network protocol, has also solved the problem. Transmitted blocks which are not acknowledged are retransmitted when a timer has run out. The protocol mechanism (only blocks received without gaps acknowledged) results in unnecessary  
20 retransmissions, depending on the round trip delay, even if the acknowledgement timeout is chosen to be long enough, since the acknowledgement timer often also runs out for messages which have been received correctly after a lost message.

25 The situation is improved somewhat by methods such as Fast Retransmission and explicit NACK upon the first occurrence of a gap.

30 The Reliable Data protocol works in a similar way to TCP, with the extension that messages which are not received without gaps can also be acknowledged.

3. The present invention discloses how certain  
35 existing protocols can be extended/modified in order to ensure efficient, secure data transmission using transmission media/protocols in which message overhaul can take place.

In this context, the present invention is based on the realization that, for a modern protocol which is intended to work efficiently, i.e. more rapidly, using a transmission medium/protocol with possible message  
5 overhaul [lacuna] loss detection with minimization of unnecessarily transmitted information, the following properties are advantageous:

- a) multiple selective retransmission method without full dependency on a timer; specifically, the loss of  
10 an ACK should not result in retransmission,
- b) explicit status alignment between transmitter and receiver,
- c) retransmission of a message only if there is a certain probability that the message is lost,
- 15 d) messages received a plurality of times must not cause an incorrect response,
- e) it should be possible to use parameter value selection to determine the tradeoff between rapid error correction and minimum unnecessary message  
20 transmission.

The most important of these points is point d). Specifically, there are two opportunities for messages received more than once to cause incorrect responses:

- 25 i) the message is recognized as having already been received, and this is defined as an error in accordance with the protocol
- ii) the message is interpreted as a new message and triggers an action which later results in an error  
30 being detected in a transmitter or receiver as a consequence. By way of example, a supposed message loss may be detected by virtue of such a message. This results in a retransmission request for messages which have not actually been sent yet, which is interpreted  
35 as an error by the transmitter.

One option for guaranteeing item d) in protocols which satisfy the other items sufficiently, but not item d),

is for a message transmitted for the second time or more to be specially marked. Such



protocols can then easily be changed so that such messages are simply ignored in the situations described under i) and ii).

5 Another opportunity to eliminate situation i) is to ignore such messages as a general rule.

For ii), a window could also be defined, so that messages received outside of this window are generally ignored and do not result in any retransmission  
10 requests.

4. The exemplary embodiment chosen is the protocol (SSCOP) described in Q.2110. This protocol fulfills the properties 3a, 3b and 3c, but has the problems  
15 described under 3i) and 3ii). Specifically, 3i) results in an incorrect response (branch to the connector D) in Q.2110, figure 20 (sheet 40 of 51). Similarly, figure 20 (sheet 40 of 51) in Q.2110 shows that a message having the property presupposed in 3ii) usually results  
20 in a retransmission request (USTAT). This in turn usually results in a branch to the error branch (connector D) in figure 20 (sheet 43 of 51).

In one embodiment of the invention, in accordance with  
25 3), an SD-PDU is now specially marked in the case of repeated transmission, e.g. by setting bit 5 in the PDU trailer (cf. figure 3/Q.2110) to 1. Figure 20 (sheet 40 of 51) in Q.2110 is modified such that, in the two error situations described above, a check is first  
30 carried out to determine whether the SD-PDU is marked as having been repeated. In this case, the message is ignored and an incorrect response cannot occur.

Alternatively, figure 20 (sheet 40 of 51) in Q.2110 is  
35 modified such that the error case 3i) is generally not checked, and a message which has already been received is simply ignored. In addition, likewise in figure 20 (sheet 40 of 51),

after the query  $VR(H) < VR(MR)$ , a check is carried out to determine whether  $SD.N(S) < VR(R) + 2^{**}23$ , for example. (This presupposes that the window size used for the flow control is always smaller than  $2^{**}23$ ,  
5 which does not represent any relevant restriction, however). If this is not the case, the message is discarded, otherwise it is handled as previously.

Item e) can also easily be achieved with SSCOP, e.g.  
10 USTATs could be sent only with a certain time delay, in order to wait for messages which have been repeated. In addition, it would be possible for only gaps which have already existed for a certain time to be reported (or heeded) using/in the case of a STAT.

15

## Patent Claims

1. A method of secure data transmission which is executed on a layer basis using a transmission method with possible message overhaul,  
5 characterized in that
- a) a message which is already being transmitted for at least the second time is specially marked by the transmitter,
  - 10 b) a message which is marked as having been transmitted for at least the second time is ignored by the receiver if it recognizes the message as having already been received or if it interprets the message as a new message.
- 15
2. A transmitter protocol which operates on a layer basis using a transmitter protocol with possible message overhaul,  
characterized in that
- 20 it specially marks a message which is already being transmitted for at least the second time.
3. A receiver protocol which operates on a layer basis using a receiver protocol with possible message  
25 overhaul,  
characterized in that
- it ignores a message which is marked as having been transmitted at least for the second time if it recognizes the message as having already been received  
30 or if it interprets the message as a new message.

4. A receiver protocol which operates on a layer basis using a receiver protocol with possible message overhaul,  
characterized in that
- 5 it ignores a message if it recognizes the message as having already been received or if, although it interprets the message as a new message, this message is situated outside of a prescribed window.

98 P 5890 DE

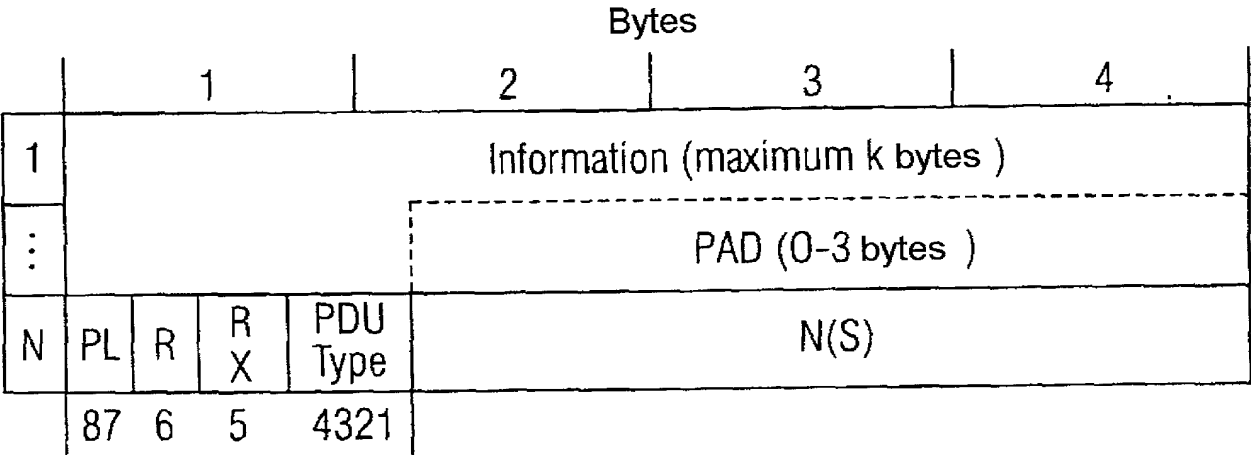
## Abstract

The invention shows how certain existing protocols can be enlarged/modified in order to guarantee an efficient, secure data transmission via transmission media/protocols, whereby message overhaul can occur.

The invention relates to a method by means of which a message, which has been transmitted for at least the second time, is particularly marked by the transmitter. The message which is marked as transmitted for at least the second time is ignored by the receiver when said message has already been received or is new.

DE 5890 DE 5890

FIG 1  
Method 1



R - Reserved  
RX - Retransmission indication

FIGURE 3/Q.2110  
Sequenced Data PDU (SD PDU)

2/11

FIG 2

Bytes			
	1	2	3
1	Reserved	N(PS)	
2	Reserved	PDU Type	N(S)
	8765	4321	

FIGURE 4/Q.2110  
Poll PDU (POLL PDU)

FIG 3

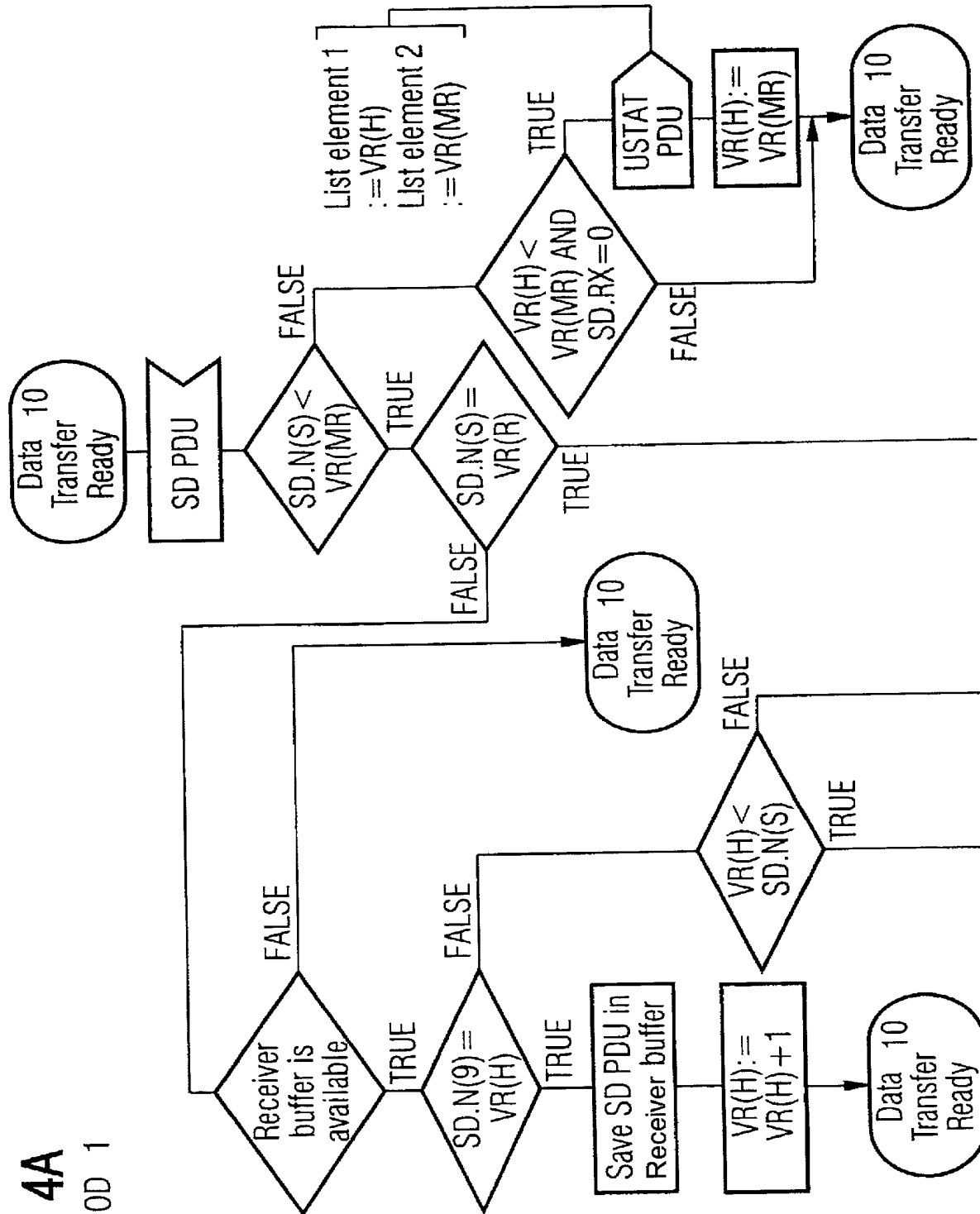
Bytes			
	1	2	3
1	PAD	List element 1 (a SD PDU N(S))	
2	PAD	List element 2	
:	:	:	
L	PAD	List element L	
L+1	Rsvd	N(PS)	
L+2	Rsvd	N(MR)	
L+3	Reserved	PDU Type	N(R)
	8765	4321	

FIGURE 5/Q.2110  
Solicited status PDU (STAT PDU)

09/857153

3/11

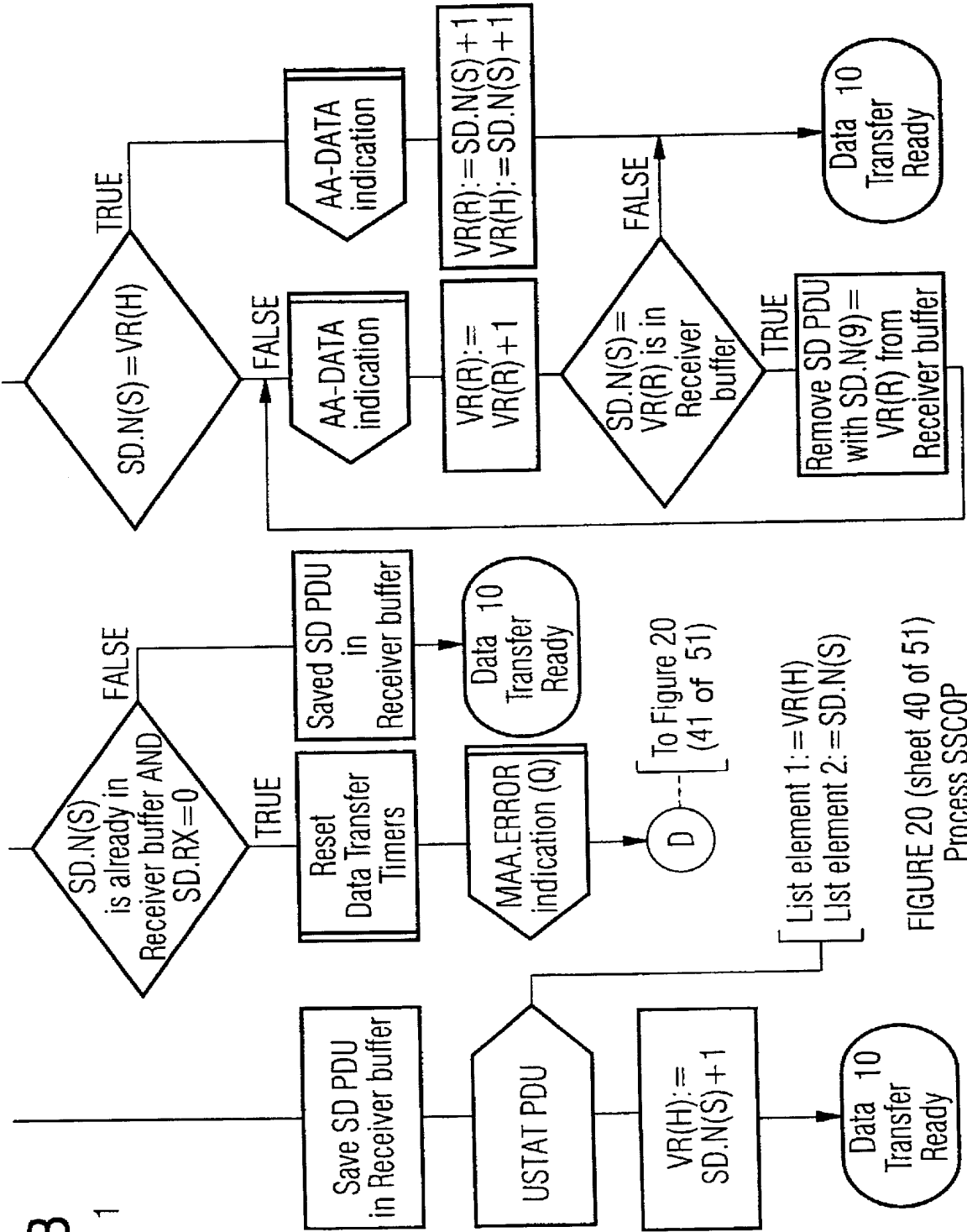
**FIG 4A**  
METHOD 1





4/11

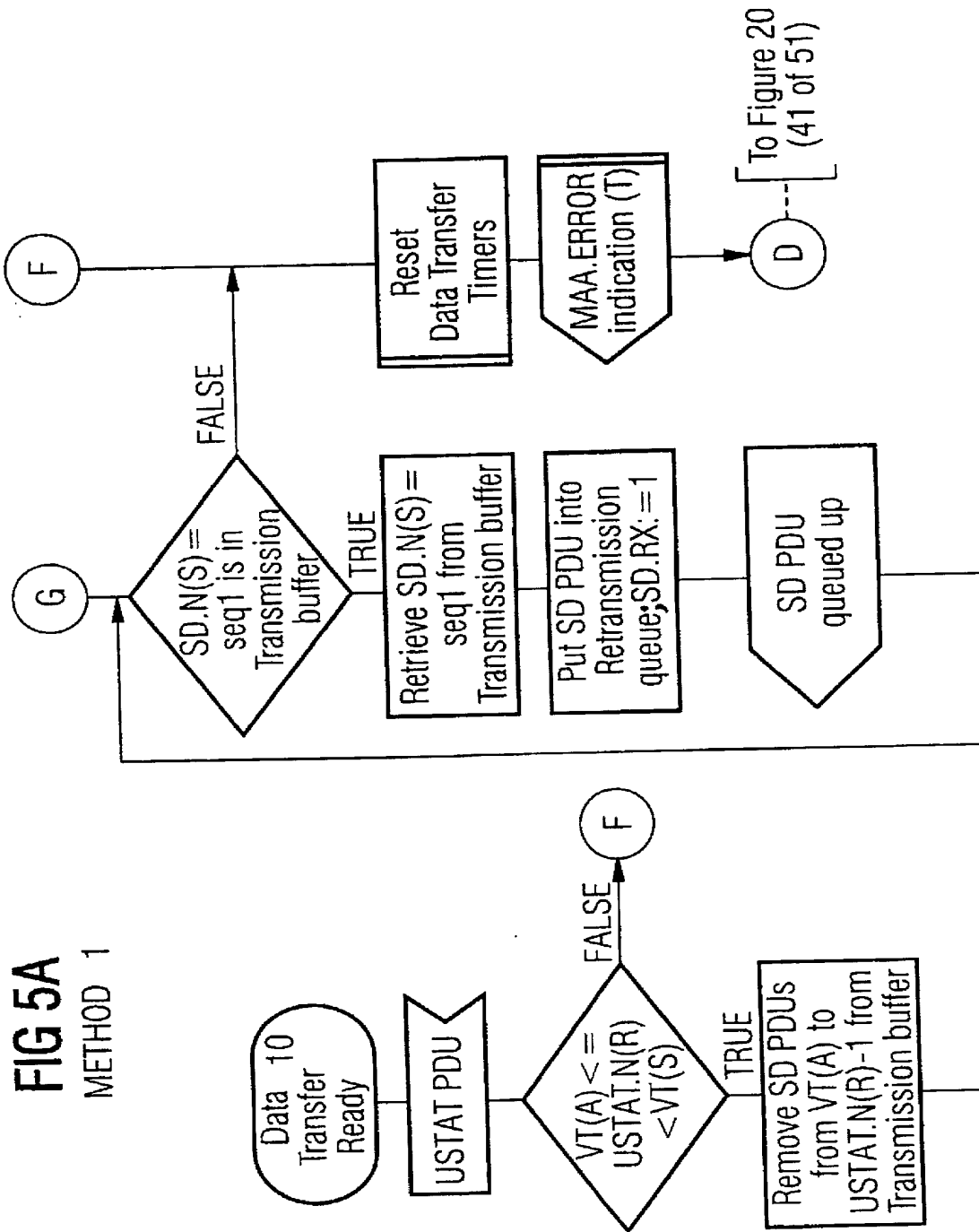
**FIG 4B**  
METHOD 1



**FIGURE 20** (sheet 40 of 51)  
Process SSCOP

5/11

**FIG 5A**  
METHOD 1



# FIG 5B

METHOD 1

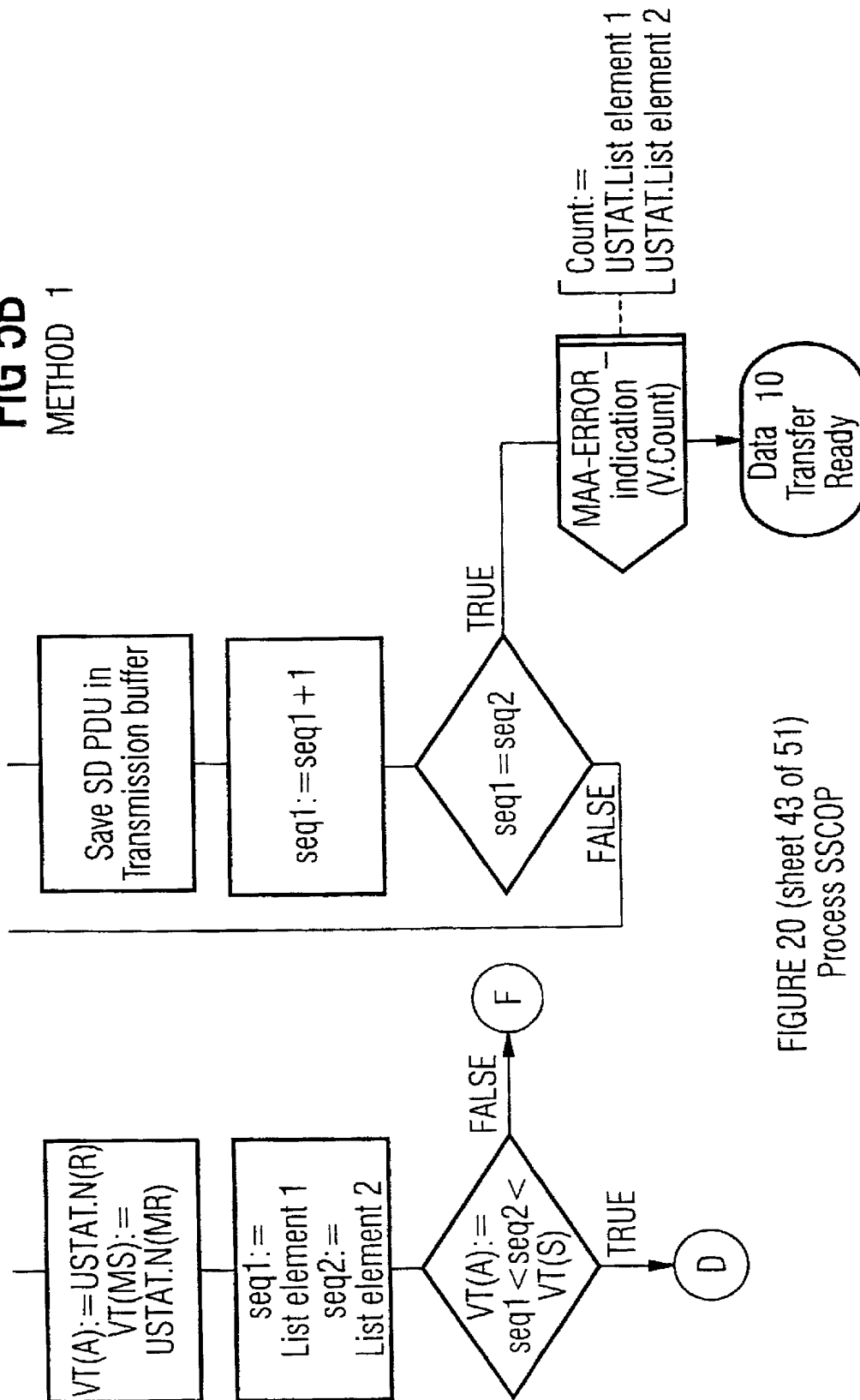
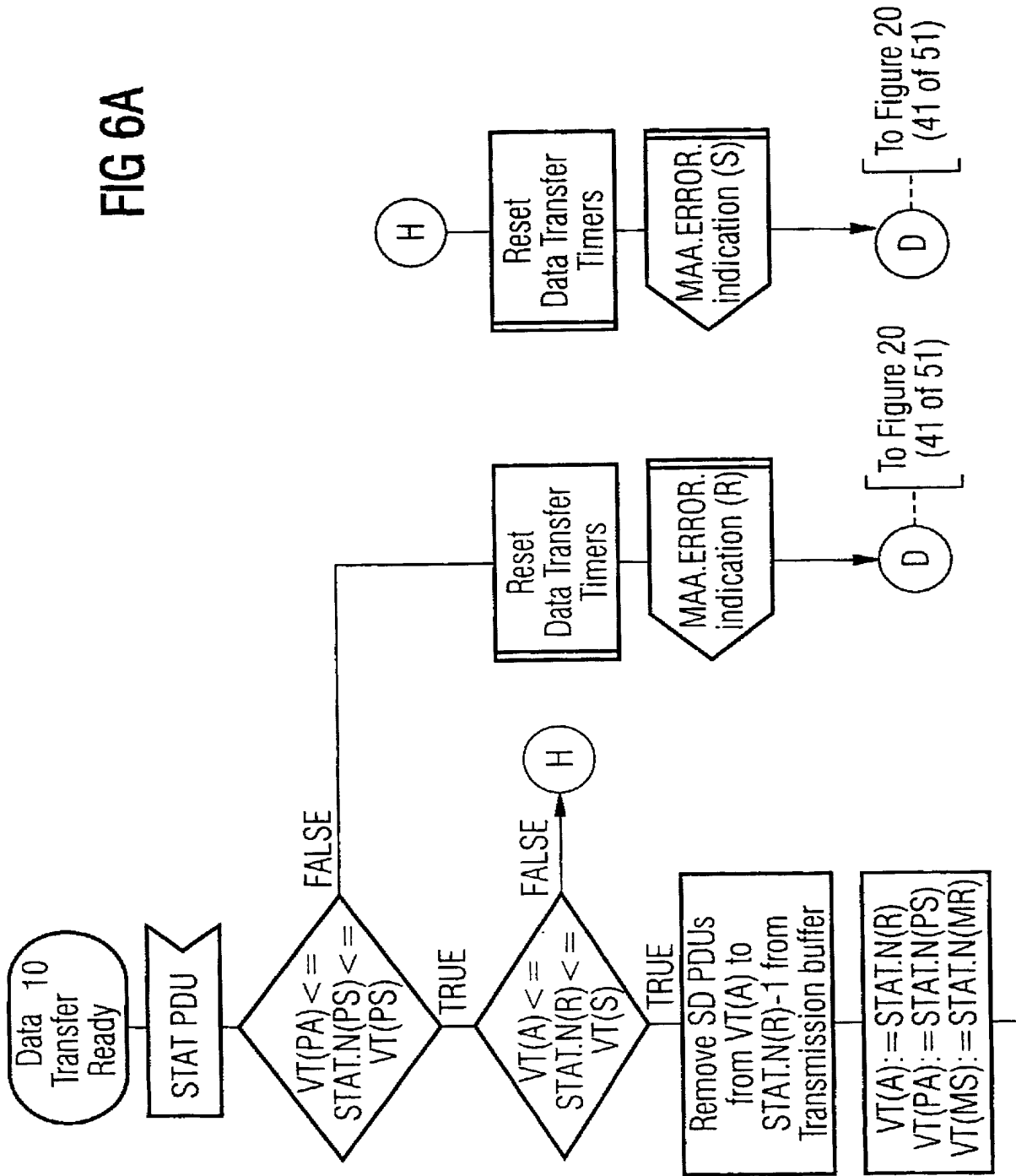


FIGURE 20 (sheet 43 of 51)  
Process SSCOP

FIG 6A



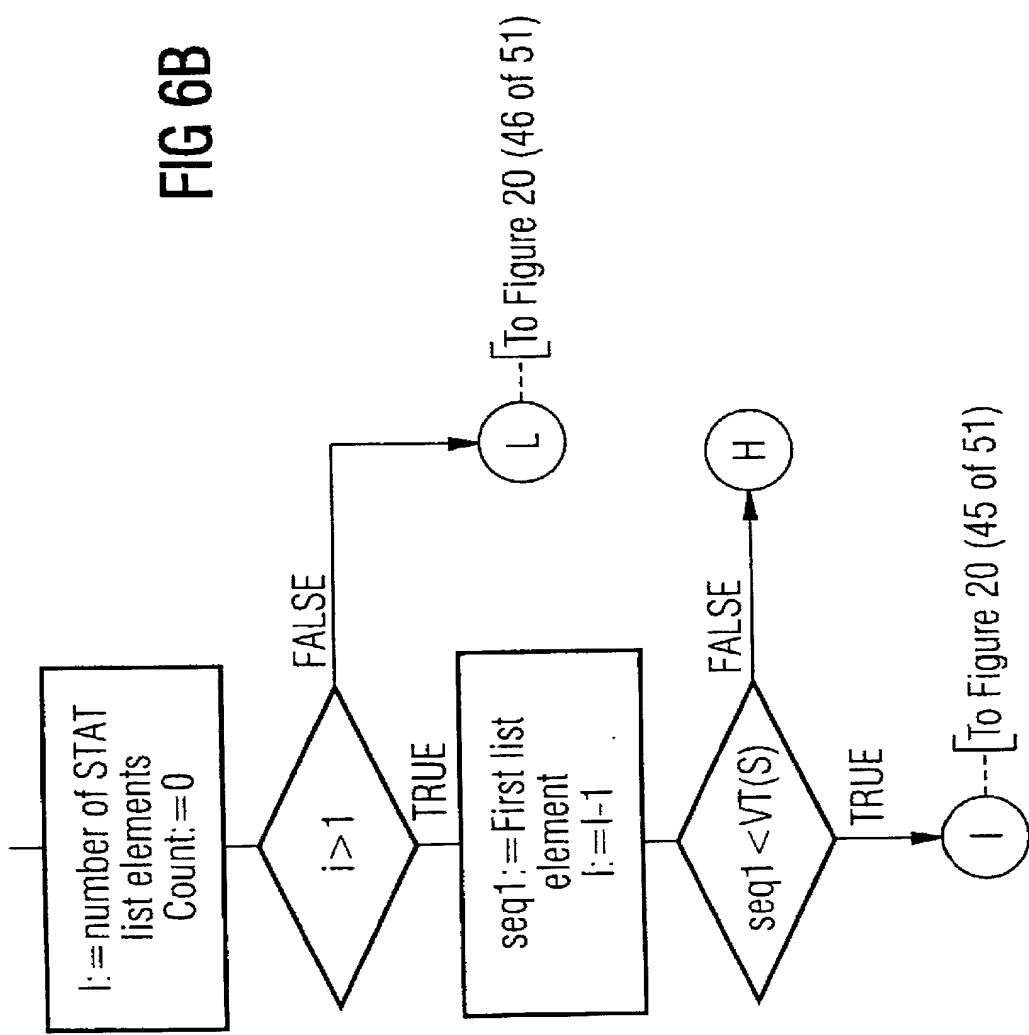


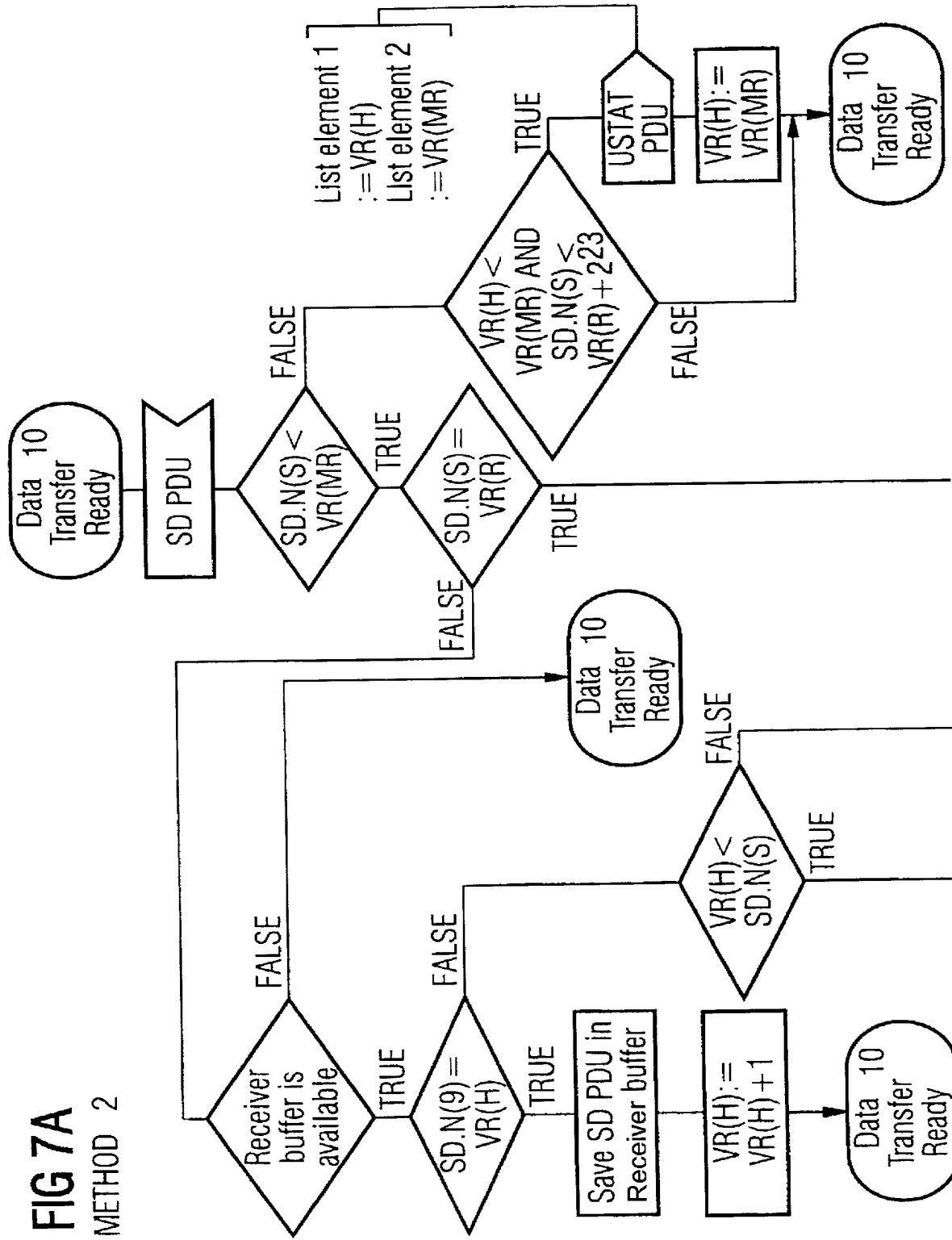
FIG 6B

FIGURE 20 (sheet 44 of 51)  
Process SSCOP

9/11

FIG 7A

METHOD 2



10/11

**FIG 7B**  
METHOD 2

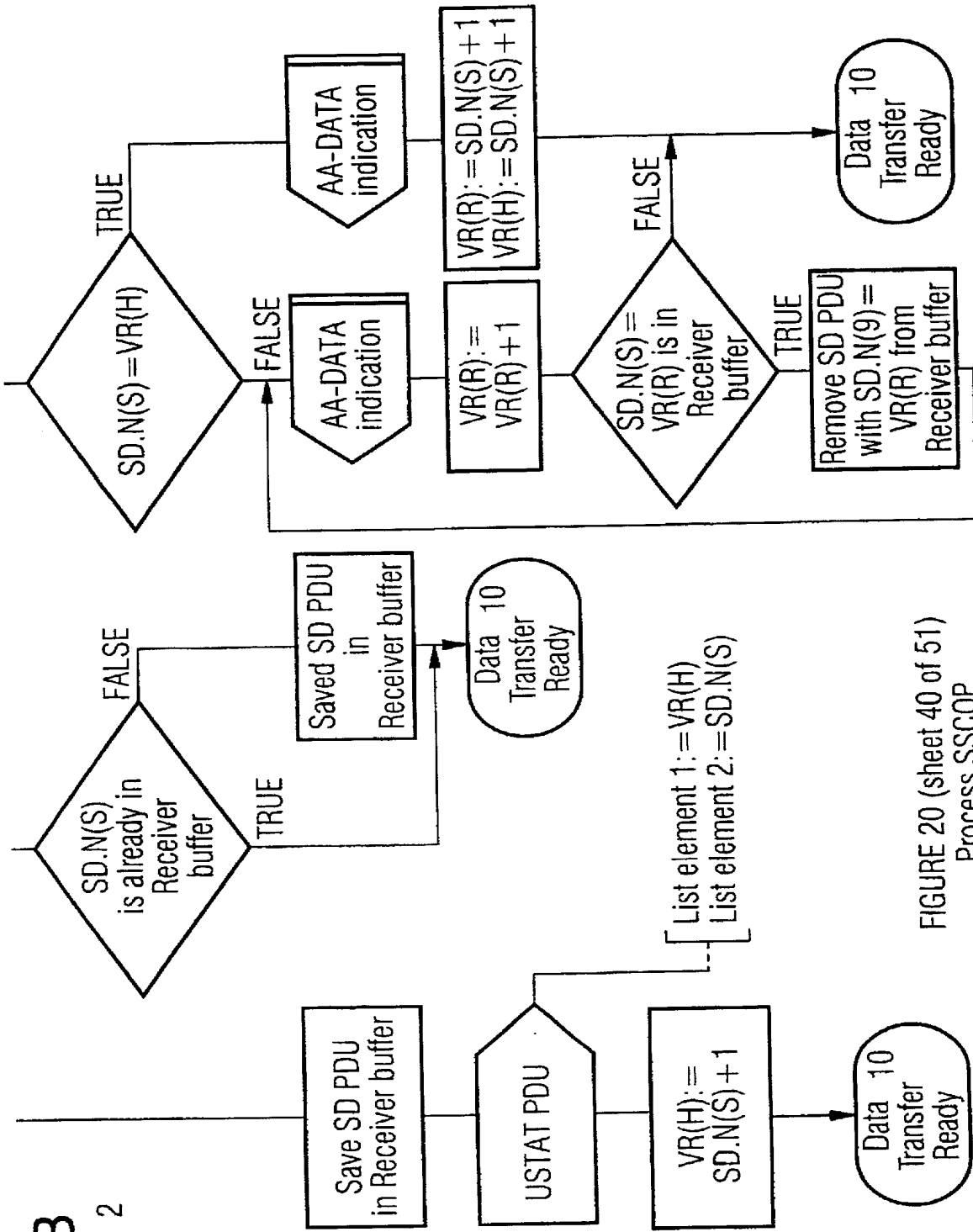
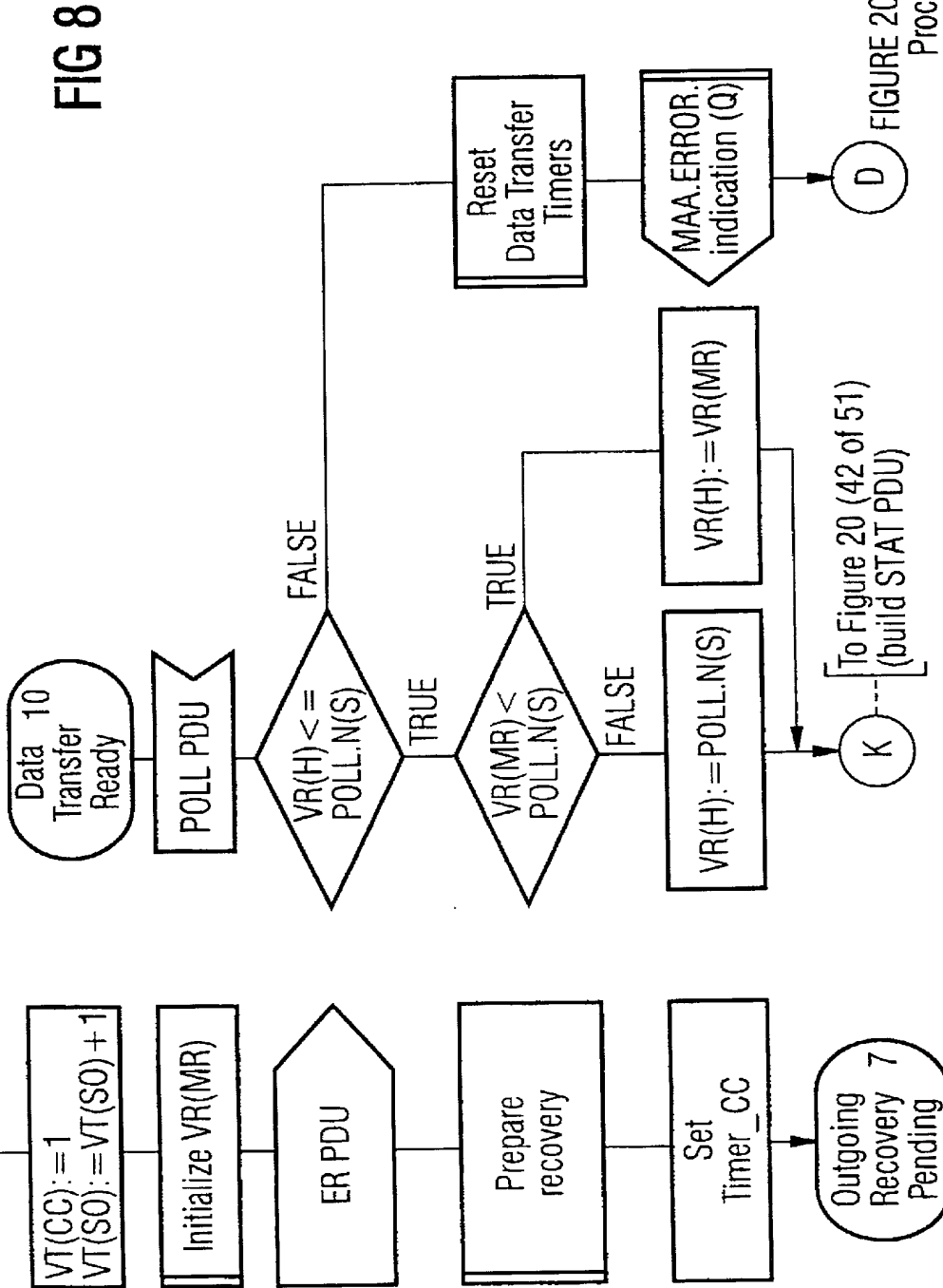


FIGURE 20 (sheet 40 of 51)  
Process SSCOP

[From Figure 20 (40, 41, 43 and 44 of 51)  
Start error recovery procedures





# German Language Declaration

Prior foreign applications  
Priorität beansprucht

Priority Claimed

198 95 6078.8      Germany      04. Dezember 1998  
(Number)      (Country)      (Day Month Year Filed)  
(Nummer)      (Land)      (Tag Monat Jahr eingereicht)

☒      ☐  
Yes      No  
Ja      Nein

(Number)      (Country)      (Day Month Year Filed)  
(Nummer)      (Land)      (Tag Monat Jahr eingereicht)

☐      ☐  
Yes      No  
Ja      Nein

(Number)      (Country)      (Day Month Year Filed)  
(Nummer)      (Land)      (Tag Monat Jahr eingereicht)

☐      ☐  
Yes      No  
Ja      Nein

Ich beanspruche hiermit gemäss Absatz 35 der Zivilprozessordnung der Vereinigten Staaten, Paragraph 120, den Vorzug aller unten aufgeführten Anmeldungen und falls der Gegenstand aus jedem Anspruch dieser Anmeldung nicht in einer früheren amerikanischen Patentanmeldung laut dem ersten Paragraphen des Absatzes 35 der Zivilprozessordnung der Vereinigten Staaten, Paragraph 122 offenbart ist, erkenne ich gemäss Absatz 37, Bundesgesetzbuch, Paragraph 1.56(a) meine Pflicht zur Offenbarung von Informationen an, die zwischen dem Anmeldedatum der früheren Anmeldung und dem nationalen oder PCT internationalen Anmeldedatum dieser Anmeldung bekannt geworden sind.

I hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, §122, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application

(Application Serial No.)  
(Anmeldeseriennummer)

(Filing Date)  
(Anmeldedatum)

(Status)  
(patentiert, anhängig,  
aufgegeben)

(Status)  
(patented, pending,  
abandoned)

(Application Serial No.)  
(Anmeldeseriennummer)

(Filing Date)  
(Anmeldedatum)

(Status)  
(patentiert, anhängig,  
aufgeben)

(Status)  
(patented, pending,  
abandoned)

Ich erkläre hiermit, dass alle von mir in der vorliegenden Erklärung gemachten Angaben nach meinem besten Wissen und Gewissen der vollen Wahrheit entsprechen, und dass ich diese eidesstattliche Erklärung in Kenntnis dessen abgebe, dass wissentlich und vorsätzlich falsche Angaben gemäss Paragraph 1001, Absatz 18 der Zivilprozessordnung der Vereinigten Staaten von Amerika mit Geldstrafe belegt und/oder Gefängnis bestraft werden können, und dass derartig wissentlich und vorsätzlich falsche Angaben die Gültigkeit der vorliegenden Patentanmeldung oder eines darauf erteilten Patentes gefährden können.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true, and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

# Declaration and Power of Attorney For Patent Application

## *Erklärung Für Patentanmeldungen Mit Vollmacht*

### German Language Declaration

Als nachstehend benannter Erfinder erkläre ich hiermit an Eides Statt:

As a below named inventor, I hereby declare that:

dass mein Wohnsitz, meine Postanschrift, und meine Staatsangehörigkeit den im Nachstehenden nach meinem Namen aufgeführten Angaben entsprechen,

My residence, post office address and citizenship are as stated below next to my name,

dass ich, nach bestem Wissen der ursprüngliche, erste und alleinige Erfinder (falls nachstehend nur ein Name angegeben ist) oder ein ursprünglicher, erster und Miterfinder (falls nachstehend mehrere Namen aufgeführt sind) des Gegenstandes bin, für den dieser Antrag gestellt wird und für den ein Patent beantragt wird für die Erfindung mit dem Titel:

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

#### Verfahren zur gesicherten Datenübertragung

---

---

---

---

deren Beschreibung

the specification of which

(zutreffendes ankreuzen)

(check one)

☒ hier beigefügt ist.

☐ is attached hereto

☐ am \_\_\_\_\_ als

☐ was filed on \_\_\_\_\_ as

PCT internationale Anmeldung

PCT international application

PCT Anwendungsnummer \_\_\_\_\_

PCT Application No. \_\_\_\_\_

Eingereicht wurde und am \_\_\_\_\_

and was amended on \_\_\_\_\_

Abgeändert wurde (falls tatsächlich abgeändert).

(if applicable)

Ich bestätige hiermit, dass ich den Inhalt der obigen Patentanmeldung einschliesslich der Ansprüche durchgesehen und verstanden habe, die eventuell durch einen Zusatzantrag wie oben erwähnt abgeändert wurde.

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims as amended by any amendment referred to above.

Ich erkenne meine Pflicht zur Offenbarung irgendwelcher Informationen, die für die Prüfung der vorliegenden Anmeldung in Einklang mit Absatz 37, Bundesgesetzbuch, Paragraph 1.56(a) von Wichtigkeit sind, an.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, §1.56(a).

Ich beanspruche hiermit ausländische Prioritätsvorteile gemäss Abschnitt 35 der Zivilprozessordnung der Vereinigten Staaten, Paragraph 119 aller unten angegebenen Auslandsanmeldungen für ein Patent oder eine Erfindersurkunde, und habe auch alle Auslandsanmeldungen für ein Patent oder eine Erfindersurkunde nachstehend gekennzeichnet, die ein Anmeldedatum haben, das vor dem Anmeldedatum der Anmeldung liegt, für die Priorität beansprucht wird.

I hereby claim foreign priority benefits under Title 35, United States Code, §119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

BOX PCT  
IN THE UNITED STATES DESIGNATED/ELECTED OFFICE  
OF THE UNITED STATES PATENT AND TRADEMARK OFFICE  
UNDER THE PATENT COOPERATION TREATY-CHAPTER II

CHANGE OF ADDRESS OF APPLICANTS' REPRESENTATIVE

APPLICANT(S): Klaus David GRADISCHNIG et al  
ATTORNEY DOCKET NO.: P01,0183  
INTERNATIONAL APPLICATION NO: PCT/EP99/09496  
INTERNATIONAL FILING DATE: 04 December 1999  
INVENTION: METHOD OF SECURE DATA TRANSMISSION

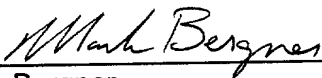
Assistant Commissioner for Patents,  
Washington D.C. 20231

S I R:

Members of the firm of Hill & Simpson designated on the original Power of Attorney have merged into the firm of Schiff Hardin & Waite. All future correspondence for the above-referenced application therefore should be sent to the following address:

**SCHIFF HARDIN & WAITE**  
**Patent Department**  
**6600 Sears Tower**  
**233 South Wacker Drive**  
**Chicago, Illinois 60606-6473**  
**CUSTOMER NUMBER 26574**

Submitted by,

  
\_\_\_\_\_  
Mark Bergner (Reg. No. 45,877)  
SCHIFF HARDIN & WAITE  
Patent Department  
6600 Sears Tower  
Chicago, Illinois 60606-6473  
Telephone: (312) 258-5779  
Attorneys for Applicants  
CUSTOMER NUMBER 26574

## German Language Declaration

VERTRETUNGSVOLLMACHT: Als benannter Erfinder beauftrage ich hiermit den nachstehend benannten Patentanwalt (oder die nachstehend benannten Patentanwälte) und/oder Patent-Agenten mit der Verfolgung der vorliegenden Patentanmeldung sowie mit der Abwicklung aller damit verbundenen Geschäfte vor dem Patent- und Warenzeichenamt: (Name und Registrationsnummer anführen)

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith. (list name and registration number)

And I hereby appoint

Messrs. John D. Simpson (Registration No. 19,842), Lewis T. Steadman (17,074), William C. Stueber (16,453), P. Phillips Connor (19,259), Dennis A. Gross (24,410), Marvin Moody (16,549), Steven H. Noll (28,982), Brett A. Valiquet (27,841), Thomas I. Ross (29,275), Kevin W. Guynn (29,927), Edward A. Lehmann (22,312), James D. Hobart (24,149), Robert M. Barrett (30,142), James Van Santen (16,584), J. Arthur Gross (13,615), Richard J. Schwarz (13,472) and Melvin A. Robinson (31,870), David R. Metzger (32,919), John R. Garrett (27,888) all members of the firm of Hill, Steadman & Simpson, A Professional Corporation.

Telefongespräche bitte richten an:  
(Name und Telefonnummer)



Direct Telephone Calls to: (name and telephone number)

312/876-0200  
Ext. \_\_\_\_\_

Postanschrift:

Send Correspondence to:

**HILL, STEADMAN & SIMPSON**  
A Professional Corporation  
85th Floor Sears Tower, Chicago, Illinois 60606

Voller Name des einzigen oder ursprünglichen Erfinders: <b>GRADISCHNIG, Klaus David</b> 10.1.2000		Full name of sole or first inventor:	
Unterschrift des Erfinders 	Datum 10.1.2000	Inventor's signature	Date
Wohnsitz D-82131 Gauting, Germany		Residence	
Staatsangehörigkeit Bundesrepublik Deutschland		Citizenship	
Postanschrift Max-Klinger-Str. 28		Post Office Address	
D-82131 Gauting			
Bundesrepublik Deutschland			
Voller Name des zweiten Miterfinders (falls zutreffend): <b>SCHWARZBAUER, Hanns</b>		Full name of second joint inventor, if any:	
Unterschrift des Erfinders 	Datum 10.1.2000	Second Inventor's signature	Date
Wohnsitz D-82194 Gröbenzell, Germany		Residence	
Staatsangehörigkeit Bundesrepublik Deutschland		Citizenship	
Postanschrift Edelweissstrasse 2A		Post Office Address	
D-82194 Gröbenzell			
Bundesrepublik Deutschland			

(Bitte entsprechende Informationen und Unterschriften im Falle von dritten und weiteren Miterfindern angeben).

(Supply similar information and signature for third and subsequent joint inventors).

300

Voller Name des dritten Miterfinders: <b>TÜXEN, Michael</b>		Full name of third joint inventor.	
Unterschrift des Erfinders <i>Michael Tuxen</i>	Datum <i>10.1.2000</i>	Inventor's signature	Date
Wohnsitz <b>D-81479 München, Germany</b> <i>DEX</i>		Residence	
Staatsangehörigkeit <b>Bundesrepublik Deutschland</b>		Citizenship	
Postanschrift <b>Gasparistr. 8</b>		Post Office Address	
<b>D-81479 München</b>			
<b>Bundesrepublik Deutschland</b>			
Voller Name des vierten Miterfinders (falls zutreffend):		Full name of fourth joint inventor, if any:	
Unterschrift des Erfinders	Datum	Inventor's signature	Date
Wohnsitz		Residence	
Staatsangehörigkeit		Citizenship	
Postanschrift		Post Office Address	
Voller Name des fünften Miterfinders (falls zutreffend):		Full name of fifth joint inventor, if any:	
Unterschrift des Erfinders	Datum	Inventor's signature	Date
Wohnsitz		Residence	
Staatsangehörigkeit		Citizenship	
Postanschrift		Post Office Address	
Voller Name des sechsten Miterfinders (falls zutreffend):		Full name of sixth joint inventor, if any:	
Unterschrift des Erfinders	Datum	Inventor's signature	Date
Wohnsitz		Residence	
Staatsangehörigkeit		Citizenship	
Postanschrift		Post Office Address	

(Bitte entsprechende Informationen und Unterschriften im Falle von dritten und weiteren Miterfindern angeben).

(Supply similar information and signature for third and subsequent joint inventors).